

[| NODIS Library](#) | [| Organization and Administration\(1000s\)](#) | [| Search](#) |

NASA Procedural Requirements

NPR 1600.2Effective Date: October 11,
2011Expiration Date: October 11,
2016**COMPLIANCE IS MANDATORY**

NASA Classified National Security Information (CNSI) w/Change 2 (2/12/2014)

Responsible Office: Office of Protective Services

Change Number	Date	Change Description
1	11/01/2012	Updated paragraphs based on information reviewed in the NASA Far Supplement.
2	2/12/2014	"Center Chief of Security" has been updated to be consistent with other Office of Protective Services NPRs identifying "Center Chief Protective Services/Center Chief of Security (CCPS/CCPS/CCS)". This is a global change throughout this NPR. P.4.s. - Corrected reference document Committee on National Security Systems Policy (CNSSP) Number 16, "National Policy for the Destruction of Communications Security (COMSEC) Paper Material". Sections 1.2.4 & 2.1 - Clarified Annual SF-311, SF-716 reporting requirements and Self-Inspection Program requirements. Section 2.3 - Provided clarification on Derivative Classification Training Requirements. Section 2.4 - added 3 year refresher training requirement Declassification Authorities. Section 2.30.1 - Provided clarification on Annual ISOO reporting requirements

Table of Contents

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Introduction

- 1.1 Overview
- 1.2 Responsibilities

Chapter 2. CNSI Management

- 2.1 Agency Information Security Program Data Report, SF-311
- 2.2 Original Classification and Marking
- 2.3 Derivative Classification
- 2.4 25-Year Automatic Declassification and Downgrading of CNSI
- 2.5 Access to CNSI
- 2.6 Accountability and Control of CNSI
- 2.7 Page Checks
- 2.8 Working Papers
- 2.9 Storage of CNSI, NATO, and Classified Foreign Government Material
- 2.10 Reproduction of CNSI
- 2.11 Hand-Carrying and Receipting of Classified Material
- 2.12 Transmission of Classified Material
- 2.13 Release of Classified Information to Foreign Governments
- 2.14 Receipt System
- 2.15 Managing and Handling Communications Security (COMSEC) Material and Devices
- 2.16 Defense Courier Service Reimbursement Program
- 2.17 Disposition or Destruction of Classified Material
- 2.18 Destruction Procedures
- 2.19 Security Violations and Compromise of CNSI
- 2.20 CNSI Meetings and Symposia
- 2.21 Security Containers and Vaults
- 2.22 Security Areas
- 2.23 Classified Material is NOT Personal Property
- 2.24 Security Classification Reviews for NASA Programs and Projects
- 2.25 Access to Classified National Security Information (CNSI) Granted by Another Government Agency.
- 2.26 Special Access Program (SAP)
- 2.27 Sensitive Compartmented Information Programs (SCI)
- 2.28 Industrial Security
- 2.29 Information Systems Security of CNSI
- 2.30 ISOO Reporting Requirements

Appendix A: Definitions

Appendix B: Acronyms

Appendix C: References

Preface

P.1 Purpose

- a. This NASA Procedural Requirement (NPR) establishes Agency-wide policy for the protection of Classified National Security Information (CNSI).
- b. This NPR prescribes personnel responsibilities and procedural requirements for the management of CNSI to assist NASA Centers and Component Facilities in executing the NASA security program designed to protect people, property, and information.
- c. In accordance with Classified National Security Information, Exec. Order No. 13526 and its implementing directive, Information Security Oversight Office (ISOO) Directive No. 1, 32 C.F.R. Parts 2001 and 2003, this NPR establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA.

P.2 Applicability

This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory (a Federally Funded Research and Development Center), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

P.3 Authority

The National Aeronautics and Space Act, 51 United States Code (U.S.C.) § 20132 Pub. L. No. 111-314, Dec 18, 2010.

P.4 Applicable Documents and Forms

- a. Freedom of Information Act, 5 U.S.C. 552.
- b. Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2011 et seq.
- c. Records Management by Federal Agencies, 44 U.S.C. § 2905, § 3101, and § 3102.
- d. Privacy Act of 1974, Pub. L. No. 93-579, 1974.
- e. Access to Classified Information, as amended, Exec. Order No. 12968, 60 Fed. Reg. 40245 (Aug. 7, 1995).
- f. Classified National Security Information, as amended, Exec. Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010).
- g. Information Security Program, 14 C.F.R. Part 1203. h. NASA Policy Directive (NPD) 1600.2, NASA Security Policy.
- i. NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA Installations

or Facilities by Foreign Nationals or U.S. Citizens Who Are Reps of Foreign Entities.

j. NPR 1441.1, NASA Records Retention Schedule.

k. NPR 1450.10, NASA Correspondence Management and Communications Standards and Style.

l. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

m. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.

n. NASA Central Office of Record Standard Operating Procedures (CSOP).

o. NASA Declassification Management Plan.

p. NASA Handbook for Writing Security Classification Guides.

q. NASA Special Access Program Security Guide (SAPSG).

r. Advisory Circular, "Federal Aviation Administration, Subject: Screening of Persons Carrying U.S. Classified Material, AC 108-3."

s. Committee on National Security Systems (CNSS), National Policy for the Destruction of Paper COMSEC Material, Policy No. 16.

t. ISOO Directive No. 1, 32 C.F.R Parts 2001 and 2003.

u. National Industrial Security Program Operation Manual (NISPOM) DoD 5220.22-M

v. National Security Agency (NSA)/Central Security Service Policy 9-12, Storage Device Declassification Manual.

w. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4004, Annex B.

x. NSTISSI/CNSS Information (CNSSI) 4005, Safeguarding Communication Security (COMSEC) Facilities and Materials.

y. North Atlantic Treaty Organization (NATO) Affairs Instructions 1-07.

P.5 Measurement/Verification

a. To determine Center compliance with this NPR, Center Directors and Center Chiefs of Protective Services/Chief of Security (CCPS/CCS) or their designees shall determine and document compliance by applying a verification approach, coordinated with the Office of Protective Services (OPS) that is tailored to meet the needs of the Center. The OPS will provide the Centers with an OPS Checklist to be used in conjunction with the NPR to ensure that all Center reviews will be tailored to include all steps necessary to perform a comprehensive review of all pertinent areas within a Center. The OPS surveys the Centers and conducts inspections of Center compliance and implementation. Each Center Protective Services Office will conduct audits of select organizations throughout their Center on a yearly basis to determine if Center organizations are in compliance with this NPR. If Center organizations are in compliance with this NPR, the findings will be forwarded to the Center Director and the Assistant Administrator (AA) for Protective Services no later than 45 days from the date of completion. If the Center has some areas that are not compliant with the policy, the Center will be required to submit an action plan outlining the non-compliant area along with the corrective action for compliance. The OPS will review the findings within 30 days and inform the Center of the approval or disapproval of the corrective actions. The OPS will conduct

reviews/audits of each Center at least every three years, or sooner if required, using the OPS Security Review Checklist to determine compliance with this NPR. The findings from the OPS review will be provided to the Center Director no later than 30 days after completion of the review.

b. To determine the OPS' compliance with the requirements contained in this NPR, internal and external auditors responsible for verifying Headquarters requirements and processes shall evaluate performance.

c. The ISOO maintains continuous liaison with their agency counterparts on all matters relating to the Government-wide security classification program and the National Industrial Security Program. ISOO also conducts on-site inspections and special classified document reviews to monitor agency compliance with applicable Executive Orders. Each year ISOO gathers relevant statistical data regarding each agency's security classification program. ISOO analyzes these data and reports them, along with other relevant information, in its Annual Report to the President. NASA follows ISOO guidance and is subject to ISOO inspections and reviews.

P.6 Cancellation

NPR 1600.1, NASA Security Program Procedural Requirements, Chapter 5, dated November 8, 2005.

Chapter 1. Introduction

1.1 Overview

1.1.1 NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified/non-sensitive nature with few restrictions on its use and dissemination.

1.1.2 NASA also generates, receives, stores, disseminates, and maintains CNSI under a variety of Agency programs, projects, and through partnerships and collaboration with other Federal agencies, academia, and private enterprises.

1.1.3 In accordance with Exec. Order No. 13526 and ISOO Directive No. 1, this NPR establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA.

1.1.4 Nothing in this chapter or the applicable Executive Order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act of 1974, or the National Security Act of 1947.

1.1.5 Further, this chapter defines the security review requirements for programs and projects, pursuant to NPR 7120.5 series, establishes procedures for the creation of security classification guides (SCG), as well as requirements for reviewing permanent historical documents, pursuant to Exec. Order No. 13526, as amended, and NPR 1441.1, NASA Retention Schedule, before retirement into the Federal Records Centers or the National Archives and Records Administration (NARA).

1.2 Responsibilities

1.2.1 Pursuant to Exec. Order No. 13526, the Administrator shall demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order as outlined in this section. The Administrator has designated a senior agency official (SAO) to direct and administer the information security program for managing and safeguarding CNSI in accordance with the Order.

1.2.2 The Assistant Administrator for Protective Services has been designated as the SAO responsible for providing direction and oversight for an Agency-wide administrative information security program and implementation of Aeronautics and Space Information Security Program, 14 C.F.R. Part 1203-Information Security Program, Exec. Order No. 13526, as amended, and ISOO Directive No. 1 for the protection of CNSI in NASA's custody. The AA for Protective Services shall:

- a. Establish Agency-wide procedures pertaining to the management of CNSI and material generated by or in the custody of NASA.
- b. Periodically review procedures and systems of Headquarters, Centers, (including Component Facilities), technical support centers, and service support centers to ensure CNSI are properly protected against unauthorized disclosure or access.
- c. Be responsible for the funding, maintenance, and operation of systems supporting CNSI.

1.2.3 Center Directors shall be responsible, through the respective CCPS/CCS, for ensuring proper planning and implementation of Exec. Order No. 13526 and managing classified information and material under the jurisdiction and custody of their respective Centers. This responsibility includes component activities at facilities or locations geographically separated from the parent Center.

1.2.4 The CCPS/CCS shall ensure an information security program for CNSI is developed, implemented, and maintained at a level sufficient to meet the requirements of this chapter and national-level requirements. This includes:

- a. Developing and implementing appropriate processes and procedures for classifying NASA information pursuant to Exec. Order No. 13526 and other national-level requirements.
- b. Developing and implementing appropriate processes and procedures for automatic declassification pursuant to Exec. Order No. 13526.
- c. Developing and implementing procedures for the appropriate safeguarding of CNSI.
- d. Developing and implementing an annual self-inspection program. The annual self-inspection program should evaluate the effectiveness of Center programs covering original classification, derivative classification, safeguarding (to include telecommunications, automated information systems, and network security), security violations, security education and training, and management and oversight. In addition, self-inspections include regular reviews of representative samples of Centers' original and derivative classification actions; these samples must encompass all Center activities that generate classified information. Annual self-inspection results shall be reported annually to the Director Security Management Division and will include:
 - (1) A description of Center's self-inspection program that provides an account of activities assessed, program areas covered, and methodology used.
 - (2) A summary and assessment of the findings from the self-inspection.
 - (3) Specific information from the review of Center's original and derivative classification actions.
 - (4) Actions taken or planned to correct deficiencies; and
 - (5) Best practices identified during self-inspections.
- e. Conducting regular and periodic reviews in coordination with the OPS Security Management Division Director. The CCPS/CCS shall conduct regular and periodic reviews of NASA organizational units involved in original and derivative classification work and storage of classified material to ensure compliance with Exec. Order No. 13526, 32 C.F.R, Parts 2001 and 2003, this NPR, and any applicable local procedures. Reviews shall meet the intent of ISOO Directive No.1, Subpart C and shall be reported annually on Standard Form (SF) 311, Agency Security Classification Management Program Data Form. The annual SF-311 form is used to report all classification, declassification, derivative actions, inspections, and other security-related activities at the Center. The Center Protective Services Office will complete the SF-311 and submit the completed form to the OPS. The SF-311 is not an audit. The reviews will also help to find misclassifications that need to be corrected.
- f. Losing or compromising classified information or material shall be reported immediately to the CCPS/CCS upon discovery of the incident. The Center Security Office will appoint a lead from the Center Protective Services Office to head the investigation and to contact the appropriate organizations required to complete this action.
- g. The CCPS/CCS may be required to raise the security threat level or develop temporary procedures to handle national security incidents.

h. In accordance with Exec. Order No. 13526 and ISOO Directive No. 1, NISPOM, and this NPR, the CCPS/CCS are responsible for developing and administering initial training, annual refresher training, specialized training as required, and termination briefings for all NASA civil service employees and for contractor personnel as required in accordance with an official NASA contract. The training will be developed in coordination with the OPS to ensure the minimum requirements of Federal policies are met. The training will include information, industrial, personnel, and industrial security policies and procedures.

1.2.5 NASA supervisors shall ensure that personnel entrusted with classified information attend the required briefings and security awareness training provided by the Center Protective Services Office or other Government agencies that provide classified information to NASA personnel. Individuals who handle CNSI shall be fully knowledgeable of and in compliance with the provisions set forth in this NPR and Exec. Order No. 13526, as amended, established for governing, accessing, protecting, accounting for, and safeguarding classified information and material. The management of classified information will be included in individual performance plans as a critical element as required by Section 5.4, (7) of Exec. Order No. 13526.

1.2.5.1 The Center COMSEC Officer will serve as the focal point for all COMSEC issues. The Center COMSEC Account Manager (CAM) and Alternate CAM serve as the focal point for all Center COMSEC issues.

1.2.6 All NASA and contractor personnel.

1.2.6.1 Employees entrusted with CNSI shall immediately report the following to the CCP/CCS:

- a. Loss or suspected compromise of classified information or material.
- b. Known or suspected practice or condition that compromises the proper safeguarding and handling of classified information or material.
- c. Attempts by uncleared personnel or personnel without a need-to-know to gain access to CNSI.
- d. Initial classification, downgrading, or declassification actions associated with NASA-generated information or material.

1.2.6.2 All personnel entrusted with CNSI are encouraged and expected to challenge the classification of information that they believe is improperly designated as being either classified or unclassified. Section 2.2.1.1 provides additional information. The Center Protective Services Office should be contacted for further assistance.

CHAPTER 2. CNSI Management

2.1 2.1 Agency Information Security Program Data Report, SF-311, Agency Security Classification Costs Estimates, SF-716, and Annual Self-Inspection Program.

2.1.1 Annual SF-311 reports are required at the end of each fiscal year. The reporting period is from October 1 to September 30. The CCPS/CCS shall submit a report to the OPS Security Management Division Director no later than October 15 following the reporting period.

2.1.2 Annual SF-716 cost estimates for security classification activities are required at the end of each fiscal year. The reporting period is from October 1 to September 30. The CCPS/CCS shall submit their cost estimates to the OPS Security Management Division Director no later than January 31 following the reporting period.

2.1.3 CCPS/CCS shall submit Annual Self-Inspection Program report to the OPS Security Management Division Director no later than October 1 each year.

2.2 Original Classification Authority (OCA) and Marking

2.2.1 Classification. Information is classified pursuant to Exec. Order No. 13526, as amended by an OCA and is designated and marked as Top Secret, Secret, or Confidential. Except as provided by statute, no other terms shall be used to identify classified information. Information may be originally classified under the terms of this order only if all the following conditions are met:

- a. An original classification authority is classifying the information.
- b. The information is owned by, produced by or for, or is under the control of the United States Government. If there is significant doubt about the need to classify information, it shall not be classified. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review. Classified information is not declassified automatically as a result of any unauthorized disclosure of identical or similar information. The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.
- c. The information falls within one or more of the categories of information listed in section 1.4 of the Order.
- d. The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

2.2.1.1 Classification Levels. Information may be classified at one of the following three levels:

- a. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- b. "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- c. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably

could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

2.2.1.1.1 Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

2.2.1.1.2 If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

2.2.1.1.3 Exceptional classification cases. When an employee, Government contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information is to be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency will render a decision within 30 days on whether to classify this information.

2.2.1.1.4 In some cases an aggregation of preexisting unclassified items of information may require that a classification action be initiated. This act is called compilation. Contact the Center Security Protective Service Office to determine if a classification action is warranted.

2.2.1.2 Classification Categories. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of Exec. Order No. 13526 and if it pertains to one or more of the following:

- a. Military plans, weapons systems, or operations.
- b. Foreign government information.
- c. Intelligence activities (including covert action), intelligence sources or methods, or cryptology.
- d. Foreign relations or foreign activities of the United States, including confidential sources.
- e. Scientific, technological, or economic matters relating to the national security.
- f. United States Government programs for safeguarding nuclear materials of facilities.
- g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.
- h. Development, production, or use of weapons of mass destruction.

2.2.1.3 Classification Prohibitions and Limitations. In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to prevent the following:

- a. Conceal violation of law, inefficiency, or administrative error.
- b. Prevent or delay the release of information that does not require protection in the interest of the national security.
- c. Prevent embarrassment to a person, organization, or agency.
- d. Restrain competition.
- e. Prohibit classification of basic scientific research information not clearly related to the national security.

f. Prohibit reclassification of information after declassification and release to the public under proper authority unless it is in compliance with Section 1.7 (c) - (e) of Exec. Order 13526.

2.2.1.4 Classification challenges. To challenge the classification status of information, authorized holders of the classified information shall present such challenges to the OPS Security Management Division Director. Once the challenge is received, a determination will be made to submit the challenge to an OCA with jurisdiction over the information. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified or is classified at a certain level. An attempt will be made to keep all challenges, appeals, and responses unclassified. Once the challenge is received, it will be reviewed and a determination will be made to grant in full or adjust the classification of the information. If the challenge is denied, a rationale for denial will be provided to the individual that submitted the challenge. If the individual does not agree with the denial, the challenge will be referred to the NASA Information Security Program Committee which will make the final Agency determination or refer the challenge to the ISOO if additional assistance is needed in making a final determination. Individuals are not subject to retribution for bringing such actions to the attention of the appropriate official or office. The following procedures will be followed when processing a challenge:

- a. The OPS Security Management Division Director shall provide an initial written response to a challenge within 60 days.
- b. If the OPS Security Management Division Director is unable to respond in 60 days, the challenge will be acknowledged in writing and the letter will include a response date.
- c. The challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision if no Agency response is received within 120 days.
- d. The challenger may also forward the challenge to the ISCAP if NASA has not responded to an internal appeal within 90 days of the Agency's receipt of the appeal.
- e. If a challenge is denied, the challenger will be made aware of appeal rights to ISCAP.
- f. Whenever an agency receives a classification challenge to information that has been the subject of a challenge within the past two years or that is the subject of pending litigation, that agency is not required to process the challenge. That agency is only required to inform the challenger of this fact and of the challenger's appeal rights, if any. Challengers and agencies shall attempt to handle and protect all appeals, classification challenges, and responses in accordance with the Exec. Order No. 13526 and its implementing directives. Information being challenged for classification will remain classified unless and until a final decision is made to declassify it. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status or particular information. Such informal inquiries should be encouraged as a means of minimizing the number of formal challenges.

2.2.2 Agency personnel with OCA designation are identified in 14 C.F.R, Subpart H - Delegation of Authority to Make Determinations in Original Classification Matters, Part 1203.

- a. The following NASA personnel possess OCA designation up to and including Top Secret: the NASA Administrator, Deputy Administrator, Associate Administrator, and the AA for Protective Services. All OCAs must receive training, at least annually, in proper classification (including the avoidance of over-classification) and declassification as provided in Exec. Order No. 13526 and its implementing directives. OCAs who do not receive such mandatory training shall have their classification authority suspended by the SAO until such training is completed. A waiver may be granted by the SAO if an individual is unable to receive training due to unavoidable circumstances. Whenever a waiver is granted, the individual will receive training as soon as practicable. The

Administrator and the Deputy Administrator will coordinate with the SAO before using their authority to suspend or grant a waiver for training so that appropriate records are maintained.

b. When designated in writing by the AA for Protective Services, the OPS Security Management Division Director and any other personnel with sufficient justification may possess OCA designation up to Top Secret (non-delegable).

c. When designated in writing by the AA for Protective Services, the NASA Inspector General, the CCPS/CCS, and any other personnel with sufficient justification may possess OCA designation up to Secret (non-delegable).

2.2.3 Identification and Markings for Original Classification. At the time of original classification, the following shall be indicated in a manner that is immediately apparent. These marking instructions apply to both hard copies and electronic records.

a. One of the three classification levels defined in Exec. Order No. 13526 §1.2.

b. The identity, by name and position, by personal identifier, or by the original classification authority.

c. The agency and office of origin, if not otherwise evident.

d. Declassification instructions, which shall indicate one of the following: the date or event for declassification as prescribed in section 1.5 (a) of the Order, the date that is 10 years from the date of original classification as prescribed in 1.5 (b) of the Order, or the date that is up to 25 years from the date of original classification as prescribed in section 1.5 (b) of the Order.

e. The marking prescribed in implementing directives issued pursuant to the Order, if information should clearly reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.

f. A concise reason for classification that, at minimum, cites the applicable classification categories in section 1.4 of the Executive Order. Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

g. With respect to each classified document, the agency originating the document indicates by marking or other means which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under the Order, the Director of the ISOO may grant and revoke temporary waivers of the requirement. The Director shall revoke any waiver upon a finding of abuse.

2.2.3.1 Personnel shall not designate information as classified Confidential, Secret, or Top Secret unless specifically approved by an individual having OCA.

2.2.3.1.1 Physically marking classified information with the appropriate classification markings clearly warns and informs people of their responsibility to protect it.

2.2.3.1.2 Other notations facilitate downgrading and declassification and aid in derivative classification actions.

2.2.3.2 Overall markings along with page, component, portion markings, and use of cover sheets shall conform to guidelines established by the CCPS/CCS in accordance with Exec. Order No. 13526 and promulgated in Chapter 8, "Classified Correspondence," of NPR 1450.10, NASA Correspondence Management and Communications Standards and Style. If you are required to mark documents on a classified system, piece of equipment or some other unique classified item, please contact your Center Protective Service Office for specific instructions on how to mark each item.

The Information Security Oversight Office (ISOO) Pamphlet, "Marking Classified National Security Information," also shows examples for marking classified e-mails and other devices.

2.2.3.3 Documents classified under any previous Executive Order need not be remarked to comply with current marking requirements.

2.3 Derivative Classification

2.3.1 Authorization and Training for Derivative Classifiers.

2.3.1.1 Persons authorized to perform derivative classification shall be identified in writing by the CCPS/CCS and reported annually along with the SF-311 reporting (see Section 1.2.4 d.). In addition, derivative classifiers are required to report the number of derivative classification decisions they make annually to their respective CCPS/CCS for inclusion in their SF-311 reporting.

2.3.1.2 The CCPS/CCS shall develop and issue derivative classification training in accordance with Exec. Order No. 13526 and ISOO Directive No. 1 for all individuals authorized to process derivative classification actions and procedures. Prior to performing derivative classification activities, authorized individuals shall receive training in the proper application of the derivative classification principles of Exec. Order No. 13526 and at least once every 2 years thereafter. At a minimum, this training should include:

- a. Principles of derivative classification
- b. Classification levels
- c. Duration of classification
- d. Identification and markings
- e. Avoidance of over-classification
- f. Prohibitions and limitations of classification
- g. Sanctions
- h. Classification challenges
- i. Classification guides
- j. Information sharing

2.3.1.3 Derivative classifiers who do not receive this training at least once every 2 years shall have their authority to apply derivative classification markings suspended by the SAO until the training is completed. A waiver may be granted by the SAO if an individual is unable to receive the training due to unavoidable circumstances. Whenever a waiver is granted, the individual is to receive training as soon as practicable. Individuals that apply derivative classification markings are identified by name and position or by personal identifier for each derivative classification action. Section 2.1 of Exec. Order No. 13526 contains additional instructions for derivative classification decisions. The Administrator and Deputy Administrator have the authority to suspend and waive training, but the SAO has the primary responsibility for this function.

2.3.2 Marking for Derivative Classification.

2.3.2.1 Derivative classification is the act of incorporating, paraphrasing, restating, or using in a new form, information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a

classified document or documents or a classification guide issued by an OCA. Persons who apply derivative classification markings shall observe and respect original classification decisions, and the pertinent classification and declassification markings must be carried forward to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier will carry forward the date or event for declassification that corresponds to the longest period of classification among the sources and a listing of the sources on or attached to the official file or record copy. Users can also use classification guides for derivative classifying. The Center Security Office will be prepared to provide assistance as requested. The CCPS/CCS will ensure they have access to the ISOO "Marking Classified National Security Information" pamphlet, www.archives.gov/isoo, and other guidance.

2.3.2.2 Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only," "Sensitive But Unclassified," Controlled Unclassified Information, "Limited Official Use," or "Sensitive Security Information," shall not be used to identify CNSI. Classified foreign government documents will contain the country of origin or foreign government information (FGI). If the identity of the specific government must be concealed, the document will be marked, "This Document Contains Foreign Government Information," and pertinent information marked "FGI," together with classification level. As an example, "C-FGI."

2.3.3 Mark documents containing FGI with: "This document contains (country of origin) Information." Mark the portions that contain the FGI to indicate the country of origin and the classification level. Substitute the words "Classified Foreign Government Information" or "FGI" in situations where the identity of the specific government must be concealed. If information is classified, FGI must be concealed, the markings described here shall not be used, and the document will be marked as if it were wholly of U.S. origin. The Center Security Office can provide information and pamphlets on how to properly mark all classified information.

2.3.4 Special Access Program (SAP) Markings. NASA employs SAP markings that are authorized and prescribed by the NASA SAP Security Guide concerning national security information for limiting access to cleared personnel having a need-to-know in the performance of their official duties.

2.3.5 Sensitive Compartmented Information (SCI). The NASA Special Security Office must review for appropriate classification and marking any document for interagency use (MOU/MOA, memorandum, or general correspondence) involving SCI or suspected SCI produced without the benefit of a specific classification guide.

2.3.6 Transmittal documents and Agency-prescribed special markings shall indicate on their face/cover the highest classification level of any classified information attached or enclosed. The transmittal is to also include, conspicuously, on its face/cover the following or similar instructions as appropriate:

- a. "Unclassified When Classified Enclosure Removed."
- b. "Upon Removal of Attachments, This Document Is (Classification Level)."

2.4 25-Year Automatic Declassification and Downgrading of CNSI

2.4.1 In accordance with Exec. Order No. 13526, as amended, all CNSI records that are more than 25 years old and have been determined to have permanent historical value under "Records Management by Federal Agencies," 44 U.S.C. § 2905, § 3101, and § 3102, which establish the standards for the retention of records and determine what records shall be automatically declassified on December 31 of each year, whether or not the records have been reviewed. Section 2001.30 of 32 C.F.R. Part 2001 g and h, gives more detail about the declassification of unscheduled records and

temporary records. Subsequently, all classified records will be automatically declassified on December 31 of the year that is 25 years from the date of its original classification unless the information falls under one of the nine exemption categories in Exec. Order No. 13526, as amended. If this occurs, a decision will be made to continue classification of the information. In accordance with this NPR and pursuant to the Atomic Energy Act of 1954, as amended, and 50 U.S.C. 435, all NASA Declassification Authorities (DCA) must attend and successfully complete the NASA/OPS approved Declassification Training Program class and the Department of Energy (DOE) training on the recognition of Restricted Data and Formerly Restricted Data (RD/FRD). Upon nomination by the AA of Protective Services or Center Director/CCPS/CCS and completion of the required NASA declassification training and DOE training, individuals may be granted DCA. Each DCA will receive a Certificate of Training approved by the OPS Security Management Division Director. Certified DCAs are required to attend refresher training every 3 years thereafter.

2.4.2 The OPS Security Management Division Director has developed the NASA Declassification Management Plan that provides the framework for NASA compliance with Section 3.3 through 3.7 of Exec. Order No. 13526, as amended. The NASA Declassification Plan shall cover the following: Purpose, Legal Basis and Authority, 25-year Automatic Declassification, Systematic Declassification Review, Mandatory Declassification Review, Declassification Review Technique, RD/FRD review, Special Media Records, Top Secret, Top Secret/SCI, SAP Material review, Classification and Declassification Guides, FGI, Declassification vs. Release, NASA Records Retention Schedule, NASA Handbook for Preparing SCG, NASA SCG, NASA OCA, NASA Declassification Authority, Major Subject Matter/Equity Headings, Classification/Declassification Glossary, 25-year Automatic Declassification Exemptions, NASA Declassification Review and Referral Handbook, Review and Referral procedures, Declassification Authorities, and NASA staff contacts. NASA DCAs will only declassify NASA-originated CNSI.

2.4.3 An Agency head may exempt a group or file series "Exempt File Series" of records from automatic declassification CNSI, if a substantial portion of the records within the file series would be expected to remain exempt based on the provisions of Exec. Order No. 13526, as amended, Section 3.3. (b) and (c). ("File series" is also described in ISOO guidance as an "integral file block.") An Agency head or SAO shall notify the Interagency Security Classification Appeals Panel and the Director of the ISOO, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) Exec. Order No. 13526, as amended, Section 3.3., that the Agency proposes to exempt from automatic declassification. File series exemptions were approved by ISOO in 1996 pursuant to the Exec. Order No. 13526, signed in December 2009, and did not have to be re-approved under Exec. Order No. 13526. File series exemption criteria include the following:

- a. A description of the information, either by reference to information in specific records or in the form of a declassification guide.
- b. An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time.
- c. Except for the identity of a confidential human source or a human intelligence source, as provided in Exec. Order No. 13526, a specific date or event for declassification of the information. The panel may direct the Agency not to exempt the information or to declassify it at an earlier date than recommended. The Agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

2.4.4 The following Agency personnel have declassification and downgrading authority.

2.4.4.1 OCAs for the Agency listed in 2.2.2 are authorized to declassify NASA-originated CNSI.

2.4.4.2 Other individuals who hold a signed letter of designation as a DCA for their directorate, office, or Center. The AA for Protective Services must sign all letters of designation.

2.4.5 When conducting yearly reviews of classified holdings for automatic declassification as required under Exec. Order No. 13526, the CCPS/CCS shall ensure declassification authority is assigned to a qualified Federal employee subject-matter expert and will assist them in declassification efforts.

2.5 Access to CNSI

2.5.1 At a minimum, NASA personnel and other individuals associated by contract or other agreement shall meet the following criteria for accessing CNSI in accordance with Access to Classified Information, as amended, Exec. Order No. 12968 and Exec. Order No. 13526:

- a. Possess a personnel security clearance commensurate with the required access.
- b. Have a justified need-to-know.
- c. Sign an official nondisclosure statement (SF 312) witnessed by a NASA security official, an approved facility security officer, or other approved official.

2.6 Accountability and Control of CNSI

2.6.1 Accountability of Top Secret classified information is essential to maintaining a history of what classified material the Center has on site, where it is stored on the Center, and what cleared civil service employee or contractor has it. Through effective accounting procedures, it must be possible to trace the movement and detect the loss of classified information immediately.

2.6.1.1 All information shall be strictly accounted for and covered by a continuous chain of signature receipts. This chapter details the minimum requirements for accountability and control. Centers are encouraged to implement additional controls when appropriate.

2.6.1.2 Each Center shall have an information management system and set of written procedures to control the classified information in its possession. The system or procedures will contain specific requirements for accounting and safeguarding CNSI. The system will be sufficient to reasonably preclude the possibility of the loss or compromise of CNSI.

2.6.2 A trained Top Secret Control Officer (TSCO) and alternate shall be designated, in writing, by the CCPS/CCS. The TSCO will ensure that all Center Top Secret material is accounted for, protected, and transmitted under a chain of receipts using NASA Form 387, "Classified Material Receipt," or other Office of Protective Services approved documentation, identifying each individual with custody of the material.

2.6.3 A trained Classified Material Control Officer (CMCO) and alternate shall be designated in writing by the CCPS/CCS. The CMCO will ensure that all Center CNSI material is received by an authorized person and safeguarded in accordance with Exec. Order No. 13526, as amended, and by this NPR.

2.6.3.1 The CMCO is responsible to the CCPS/CCS for the Center Security Control Point (SCP) and oversight of the Document Control Points (DCP) within the Center and/or facilities.

2.6.3.2 Establishment of SCP. One SCP, operated by the CMCO, shall be established within each Center or facility that has a requirement to handle classified information. The SCP will be designated in writing within the local security procedural requirements. All incoming and outgoing

classified information will be processed through the SCP with the following exceptions: SCI material and classified messages that are handled, processed, and stored within secure telecommunications spaces.

2.6.3.3 DCP. At a Center with a significant volume of classified material and where the SCP serves many organizations, each organization which has or shall have custody of classified material will establish a Document Control Station Official (DCSO) run by a Document Control Point Officer. Organizationally, this station may be established at the office, division, staff, or lower level, depending upon the circumstances. Creation of such stations will be coordinated with the CMCO and approved in writing by the CCPS/CCS.

2.6.4 Accountability records.

2.6.4.1 All Top Secret material must be accounted for throughout its life cycle. Records shall be maintained for all Top Secret material and retained for five years after final disposition. These records will be maintained at the SCP for any accountable information, which is received, generated, reproduced, transmitted, downgraded, or destroyed. A Classified Document Control Log will be used for this purpose.

2.6.4.2 The Classified Document Control Log maintained at the SCP shall, at a minimum, reflect the following for Top Secret:

- a. Date of receipt and date of origination.
- b. Agency/installation from which received or by which originated.
- c. Classification level of the material.
- d. A brief unclassified title or description of the material.
- e. The date of declassification or downgrading.
- f. Control number assigned. Each copy of a classified document or item shall have its own control number. Copy numbers will not be used as part of the control number.
- g. Information indicating the location or local holder of the material. (Local holders/custodians shall have some form of signature receipt on file acknowledging that they have custody of the material.)
- h. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the installation.

2.6.4.3 The Classified Document Control Log maintained at the DCSO shall, at a minimum, reflect the following:

- a. Classification level of the material.
- b. Control number assigned.
- c. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the DCSO.

2.6.4.4 Accountability records shall contain signed receipts and destruction reports. Signed receipts and destruction reports shall be retained for five years after final disposition.

2.6.5 Top Secret disclosure records.

2.6.5.1 A disclosure record of all persons who are afforded access (including visual, oral, and record copies) to Top Secret information (except safe combinations) shall be maintained. This record will

show the names of all individuals given access and the date of such access. To comply with this requirement, a Top Secret Cover Sheet (Form SF 703) will be attached to all Top Secret information in document form. For access given orally, a log listing the required information will be maintained. At a minimum, the Disclosure Record Sheet shall provide:

- a. Information reflecting the document being disclosed.
- b. Individual to whom the information is being disclosed.
- c. Organization and telephone number.
- d. Date the information is disclosed.

2.6.5.2 Records shall be retained for five years from the date of final disposition.

2.6.6 Guidelines for Electronic Classified Information Processing.

2.6.6.1 Electronic Processing. Each Center is responsible for providing a count of all original and derivative classification actions processed throughout the year in accordance with SF-311 at the end of the fiscal year. Do not count products classified by another agency and do not count any reproductions or copies. Instruction "Guidelines for SF-311 Data Collection" should be referenced for assistance.

2.6.6.1.2 The CCPS/CCS shall establish written procedures to ensure that a record of electronic processing done throughout the year is maintained to help complete the SF-311 at the end of the fiscal year.

2.6.7 Handling of Incoming Classified Material.

2.6.7.1 The CCPS/CCS shall provide written procedures for the handling of incoming classified material. When a Center/facility receives incoming mail, bulk shipments, and items delivered by messenger, the following controls shall be implemented:

- a. All classified material shall be delivered immediately to the SCP or properly safeguarded in accordance with this NPR until delivery to the SCP can be affected.
- b. All Registered, USPS Express Mail, and contract overnight delivery packages shall be delivered unopened to the SCP and protected as Secret material until determined otherwise.
- c. All personnel who open official mail of any sort shall be directed to immediately deliver any classified material to the SCP. Outer wrappers along with the unopened inner wrapper will be delivered to the SCP. If an individual opens mail, which is not correctly packaged, causing exposure to uncleared or unauthorized individuals, the material will be delivered to the SCP, and the CCPS/CCS will be notified. The CCPS/CCS will investigate and submit a report of incidents involving classified material outlined in paragraph 2.19 of this chapter.
- d. All incoming packages containing classified material shall be inspected for tampering. If tampering is discovered, it will be reported to the CCPS/CCS who will conduct necessary inquiries. The contents of the package will be checked against the enclosed receipt.
- e. Incoming classified information that does not fall under the Classified Management Computer system, such as a large device or piece of equipment, shall be processed in accordance with the procedures established for that type of material.

2.6.8 Record of Destruction.

2.6.8.1 An accurate record of destruction of classified material is as important as the manner of its destruction. Proper accounting procedures, together with accurate records of destruction, provide

evidence of the proper disposition of classified material. Records of destruction shall be retained for five years.

2.6.8.2 A record of destruction is required for all Top Secret material designated for destruction. The destruction record shall indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness. Destruction of Top Secret material will be accomplished by at least one Center Security Specialist and one other person authorized with the need to know to access the information. Both individuals will sign the destruction receipt. Either the control log or a separate destruction report may be used for this purpose.

2.6.8.3 Secret and Confidential material shall be destroyed only by an authorized individual approved by the Center Protective Services Office.

2.6.9 Inventory requirements.

2.6.9.1 Two appropriately cleared individuals shall conduct inventories for Top Secret material. One of the individuals should be the control officer for the material.

2.6.9.2 An inventory is a visual sighting of each item of accountable material. All documents held shall be checked to ensure that they are entered into accountability, and all documents entered into accountability will be sighted, including those items signed out on local custody. If no disposition can be determined, a security incident report involving classified material will be submitted in accordance with section 2.19 of this NPR.

2.6.9.3 All Top Secret holdings shall be inventoried upon change of custodian or semiannually. Semiannual inventories may be combined with change of custodian inventories. Accountability records will also be reviewed for accuracy and continuity. Section 2.7 contains a complete listing of required page checks.

2.6.9.4 Secret and Confidential material shall be protected and safeguarded from persons without authorized access or need to know in accordance with ISOO Directive 1, Section 2001.41 and Exec. Order No. 13526.

2.6.9.5 The Center shall retain a record of all Top Secret inventories for at least five years. An inventory and a report of the results, including any discrepancies discovered, will be forwarded annually to the cognizant CCS. Although an inventory of Top Secret holdings is required on a semiannual basis, a written report to the CCPS/CCS is only required annually unless discrepancies are discovered. Although the Top Secret inventory is only reported annually, local documentation of all inventories must be maintained at the installation as described above.

2.6.9.6 Upon change of custodian, all Top Secret material shall be transferred to the new custodian. A joint inventory will be conducted, accounting for each item. Both parties will sign the report documenting the completion of the inventory.

2.6.10 Changes and corrections. The custodian, under the direction of the CMCO, shall be responsible for the entry of all changes and corrections to the material in their custody. A Publication Change Checklist must be used for all changes entered. Completed checklists will be retained until the publication is destroyed or superseded.

2.7 Page Checks

2.7.1 A page check shall be conducted on all Top Secret material. Page checks involve visually sighting each page in a document, verifying its presence against a list of effective pages (if

applicable), and ensuring that the page is from the original document. In the absence of a list of effective pages, the document will be examined for continuity. After each page check, the individual will sign the page check record (except for page checks prior to destruction). If one does not exist, a page check record will be produced locally and kept with the publication. The record will identify the publication, the name of the individual conducting the page check, discrepancies noted, and the date of the check.

2.7.2 Page checks on Top Secret material shall be conducted on the following occasions: initial receipt, page change, change residue, change of custodian, inventory, and destruction.

2.7.3 No page checks are required for Secret or Confidential material.

2.8 Working Papers

2.8.1 Working papers are documents, including drafts, notes, photographs, computer media, and any other materials accumulated, created, or received electronically that assist in the formulation and preparation of a finished document. Classifying as "working papers" is not intended as a way around the original classification procedure or temporary classification. The CCS shall be made aware of all working paper documents to ensure that the proper markings and safeguarding are being utilized to protect the information. Working papers, which contain classified information produced by a unit, will be:

- a. Dated when created.
- b. Marked with the highest classification of information contained in the document.
- c. Protected in accordance with the classification assigned.
- d. Destroyed or correctly classified by an OCA after 180 days.

2.8.2 The accounting, control, and marking requirements prescribed for a finished document shall be followed when working papers contain Top Secret information or are:

- a. Released by the originator outside the NASA facility or transmitted electronically.
- b. Retained more than 90 days from the date of origin.
- c. Filed permanently.

2.9 Storage of CNSI, NATO, and Classified Foreign Government Material

2.9.1 All classified documents and material under the jurisdiction, possession, control, and ownership of NASA shall be stored in a "General Services Administration Approved" security container with an approved combination lock or approved facility/room with sufficient physical and procedural security measures to preclude unauthorized access. Whenever new security equipment is procured, it must conform to the standards and specifications established by the Administrator of General Services and will, to the maximum extent possible, be available through the Federal Supply System. Section 2.21 contains requirements on security container management. The CCPS/CCS will ensure that adequate storage is available for CNSI in accordance with applicable NASA and Federal regulations.

2.9.2 Each Center shall apply the following:

- a. Use the SF 702-101, "Security Container Sheet."
- b. Change combinations when first placed in service and then as needed whenever a person knowing the combination is transferred or terminated from employment or is no longer authorized access to

the classified material stored in the equipment or area; whenever it is possible that the combination may have been subjected to compromise; or whenever the security storage equipment or security area has been found unsecured and unattended.

c. Safeguard NATO classified information in compliance with United States Security Authority for NATO Affairs Instructions 1-07. NATO and FGI should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. Safeguarding standards may be modified if required or permitted by treaties or agreements or for other obligations, with prior written consent of the National Security Authority of the originating government, hereafter "originating government." ISOO Directive No.1 should be referenced for more detail on how to protect FGI.

2.9.3 Senior Agency management or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations. In emergency situations in which there is an imminent threat to life or in defense of the Homeland, Agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

- a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.
- b. Limit the number of individuals who receive it.
- c. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in subpart C of ISOO Directive No.1 or other necessary means when time is of the essence.
- d. Provide instructions on safeguarding information. Physical custody of classified information must remain with an authorized Federal Government entity in all but the most extraordinary circumstances.
- e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information. Obtain a signed nondisclosure agreement.
- f. All disclosures of classified information shall be reported to the CCPS/CCS and the originator immediately or at the earliest opportunity. The CCPS/CCS will notify the OPS Security Management Division Director and provide the following information as soon as possible:
 - (1) A description of the disclosed information.
 - (2) Who authorized the disclosure.
 - (3) To whom the information was disclosed.
 - (4) How the information was disclosed and transmitted.
 - (5) Reason for the emergency release.
 - (6) How the information is being safeguarded.
 - (7) A description of the briefing provided and a copy of the signed nondisclosure agreements.

2.10 Reproduction of CNSI

2.10.1 Reproduction of classified information and material must be kept to a minimum. Only equipment designated by the CCS is authorized to reproduce classified information. Each Center

CCPS/CCS shall develop and implement written procedures to ensure that the following requirements, as a minimum, are met:

- a. Protect classified information during reproduction.
- b. Adequately clear equipment after reproduction.
- c. Ensure reproduced copies are incorporated into the Center CNSI accountability system.
- d. Safeguard overruns, waste, and blank copies generated during the clearing of reproduction equipment by handling material as "classified" and destroy copies accordingly.
- e. Ensure security procedures are provided for reproducing classified information by other technical means.

2.10.2 The CCPS/CCS shall ensure that all equipment hard drives used in machines for reproduction are wiped or destroyed in accordance with standards used to erase classified information.

2.11 Hand-Carrying and Receipting of Classified Material

2.11.1 CNSI shall be transmitted in a manner that ensures protection of the material. A receipt will be required whenever CNSI material is transmitted using an authorized NASA official, entered into the U.S. Postal System or via authorized contract courier, transmitted off the Center by any means, transmitted to a non-NASA activity, or when the transmitting custodian wishes to verify change of custody. See paragraph 2.12.1.1 for information on transmitting COMSEC information.

2.11.2 Methods of Transportation Within a Center.

2.11.2.1 The TSCO, custodian, or other employee having a Top Secret clearance and designated by either TSCO or the CCS, shall personally hand-carry Top Secret information within a Center. A Top Secret Cover Sheet (Form SF 703) will be attached to all Top Secret information in document form.

2.11.2.2 Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that timely delivery to the intended recipient is accomplished. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized to store classified information in accordance with this directive. When traveling within a building, classified material must be hand-carried, covered with the appropriate coversheet SF-703, SF-704, or SF-705 with the recipient and sender name written on the cover page, and enclosed in a single envelope or other suitable package shall be carried in a briefcase or other container. When hand-carrying classified material, the individual must proceed directly to the intended destination. Restroom breaks, coffee breaks, and any other detour, are not permitted when hand-carrying classified material.

2.11.2.3 Between buildings of a Center or outside the facility, Top Secret, Secret, and Confidential information shall be transmitted within double-wrapped, appropriately marked, and addressed envelopes with the recipient and sender address on the inner envelope with the appropriate cover sheet, SF-703, SF-704, or SF-705 attached.

2.11.2.4 Additional measures may be established by the CCPS/CCS to control access to any CNSI by an unauthorized person during transmission.

2.11.2.5 Such material shall be transmitted inside a Center by hand-delivery from an employee possessing a clearance at least as high as the category of classification of the material involved.

2.11.3 Hand-Carrying Outside a Center.

2.11.3.1 The OPS Security Management Division Director or the CCPS/CCS shall appoint a NASA

employee or contractor to be a designated courier of CNSI when it is essential for that NASA employee or contractor to hand-carry such information outside HQ or a Center.

2.11.3.2 Couriers may also be required for symposiums where transport, control, and access to CNSI may be necessary, for "cleared" conference or symposium attendees, including other Agency personnel or for NASA contractors holding NASA security clearances under a NASA DD Form 254.

2.11.3.3 Designated couriers shall be briefed by the Center Protective Services Office that classified material must be in their physical possession at all times (i.e., not in checked baggage, left unattended in a hotel room or vehicles, safeguarded in hotel safety boxes, or taken to bars, dining, or places of entertainment) and protected from opening, examination, or inspection. Furthermore, designated couriers must acknowledge that their authorization to courier CNSI is only valid within the U.S. and its Territories.

2.11.3.4 Authorization shall be provided to the designated courier on a NASA-approved Courier Authorization Card or NASA letterhead stationery, marked "Valid only in the United States of America," and will include a specific expiration date and the names and home telephone numbers of one NASA Security Specialist who may be contacted if the designated courier is challenged to open the materials by non-NASA personnel (police, other Government officials, or airline personnel). While the NASA Courier is awaiting approval to clear airport security, the classified information will be kept within an appropriate container and within the custody of the courier at all times and not opened. The NASA Security Specialist will work with the airport security manager to resolve the situation or instruct the individual to return the classified material to the Center if the situation cannot be resolved in a timely manner.

2.11.3.5 Personnel shall be briefed on Advisory Circular, "Federal Aviation Administration, Subject: Screening of Persons carrying U.S. Classified Material, AC 108-3."

2.11.3.6 CNSI transmitted outside a Center shall be enclosed in an envelope with opaque inner and outer covers. The inner cover will be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover will be sealed and addressed with no identification of the classification of its contents.

2.11.3.7 A receipt shall be attached to or enclosed in the inner cover. The receipt will identify the sender, the addressee, and a description of the materials being transmitted. The receipt will be signed by the recipient and returned to the sender, who will retain it for five years.

2.11.3.8 A suspense system shall be established to track transmitted documents until a signed copy of the receipt is returned. If signed receipts are not received within 30 days of transmission of the material, the CMCO will report the non-receipt to the CCPS/CCS.

2.11.3.9 When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit.

2.12 Transmission of Classified Material

2.12.1 The term "transmission" refers to any movement of classified material or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation is not significant.

2.12.1.1 Classified material shall be transmitted either in the custody of an appropriately cleared individual, by an approved system or courier, or otherwise in accordance with the provisions of this chapter. The NASA Central Office of Record (NASA COR) is responsible for providing instructions

concerning the transmission of Top Secret, Secret, and Confidential Communication Security (COMSEC) material, and the NASA Special Security Officer (SSO) is responsible for providing instructions concerning the transmission of Top Secret, Secret, Confidential, and Sensitive Compartmented Information (SCI) material. Contact your Center COMSEC Security Officer and your Center Special Security Officer to receive policy and guidance for COMSEC and SCI.

2.12.1.2 The carrying of classified material across national borders is not permitted unless arrangements have been made that shall preclude customs, postal, or other inspections. In addition, foreign carriers will not be used unless the U.S. escort has physical control of the classified material.

2.12.2 Top Secret transmission. Neither the normal mail nor messenger system of an installation nor postal and commercial delivery services are authorized for the transmission of Top Secret material. Top Secret material shall only be transmitted by:

- a. DCSO.
- b. Department of State Courier System.
- c. Appropriately cleared NASA civilian personnel or cleared NASA contractor specifically designated as a courier.
- d. Telecommunications systems specifically approved for transmission of Top Secret material.

2.12.3 Secret transmission. Transmission of Secret material may be effected by:

- a. Any of the means approved for the transmission of Top Secret, except that Secret material, other than that containing cryptological information, which may be introduced into the DCSO only when the control of such material cannot otherwise be maintained in U.S. custody. When the Department of State Courier System is to be used for transmission of Secret material, the Secret material shall be sent by registered mail to the State Department Pouch Room.
- b. U.S. Postal Service (USPS) registered mail within and between the 50 states and territories of the U.S.
- c. USPS Express Mail Service, which may be used between NASA units and contractors within and between the 50 United States and its Territories. USPS Express Mail is authorized only when it is the most cost effective method or when time/mission constraints require it. The package shall be properly prepared for mailing. The USPS Express Mail envelope will not serve as the outer wrapper. The package will be double wrapped as required then placed in the USPS Express Mail envelope. Under no circumstances will the sender execute the "Waiver of Signature and Indemnity" section of the USPS Express Mail Label for classified material. This action can result in drop-off of a package without the receiver's signature and possible loss of control.
- d. Federal Express (FedEx), which the CCPS/CCS may authorize for overnight delivery of material for the Executive Branch when an urgent requirement exists for overnight delivery within the 50 United States and its Territories. The sender is responsible for ensuring that an authorized person shall be available to receive the delivery. The package will only be addressed to the recipient by name. The release signature block on the receipt label will not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO, and FGI will not be transmitted in this manner.
- e. Secret material, which shall be moved by USPS registered mail through Army, Navy, or Air Force Postal Service facilities provided that the material does not pass through a foreign postal system or any foreign inspection or via foreign airlines. The material must remain under U.S. control. The Center Protective Services Information Security Specialist will ensure that classified

material sent to U.S. activities overseas will be appropriately prepared and transported by an approved carrier. If the material is introduced into a foreign postal system, it has been subjected to compromise.

f. Qualified carriers authorized to transport Secret material via a Protective Security Service under the National Industrial Security Program, within U.S. boundaries only. This method is authorized only when the size, bulk, weight, nature of the shipment, or escort considerations make the use of other means impractical.

g. Other carriers under escort of appropriately cleared personnel. The Center Protective Services Information Security Specialist will determine what carrier service should be used based on the availability of service providers in the area. Carriers include Government and Government contract vehicles, aircraft, ships of the U.S. Navy, Federal employee-manned U.S. Naval Ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships, or pilots of aircraft who are U.S. citizens may be designated as escorts, provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period if stored in an aircraft or shipped in connection with flight or sea transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons aboard or loaded in specialized shipping containers, including closed cargo containers.

h. Telecommunications systems specifically approved for the transmission of Secret material.

2.12.4 Confidential transmission. Transmission of Confidential material may be effected by:

a. Any of the means approved for the transmission of Secret material.

b. USPS registered mail.

2.12.4.1. Confidential COMSEC, NATO, and other special category material.

a. Other Confidential material to and from Fleet Post Office (FPO) or Army Post Office (APO) addressees located outside the U.S. and its Territories.

b. Other addressees when the originator is uncertain that their location is within the U.S. boundaries. Use of return postal receipts is not authorized. If considered desirable, a document receipt may be used.

c. When the sender deems it necessary to ensure adequate protection of the classified material.

2.12.4.2 USPS First Class mail between NASA and other U.S. Government agency locations anywhere in the U.S. and its territories. However, the outer envelope/wrappers of such Confidential material shall be marked "First Class," and endorsed "Return Service Requested."

2.12.4.3 Certified or, if appropriate, Registered Mail shall be used for material directed to contractors and to agencies of the Executive Branch.

2.12.4.4 Within U.S. boundaries, commercial carriers that provide a Signature Security Service. This method is authorized only when the size, bulk, weight, nature of shipment, or escort considerations make the use of other methods impractical.

2.13 Release of Classified Information to Foreign Governments

2.13.1 Subsequent to a determination by the OPS Security Management Division Director that classified material may be released to a foreign government, the material shall be transferred

between authorized representatives of each government in compliance with the provisions of this chapter. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities will either contain transmission instructions or require that a separate transportation plan be approved by the OPS Security Management Division Director prior to release of the material. Classified material must be transmitted only:

- a. To an embassy or other official agency of the recipient government that has extraterritorial status.
- b. For on-loading aboard a ship, aircraft, or other carrier designated by the recipient government at the point of departure from the U.S. or its Territories or possessions. At the time of delivery a duly authorized representative of the recipient government must be present at the point of departure to accept delivery, ensure immediate loading, and to assume security responsibility for the classified material.

2.13.2 Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee. This written designation will contain assurances that such person has a security clearance at the appropriate level and that the person will assume full security responsibility for the material on behalf of the foreign government. The recipient will be required to execute a receipt for the material, regardless of the level of classification.

2.13.3 Each contract, agreement, or arrangement, which contemplates transfer of U.S. classified material to a foreign government within the U.S. or its Territories, shall designate a point of delivery in accordance with subparagraph 2.13.1.a. or 2.13.1.b. If delivery is to be made at a point described in subparagraph 2.13.1.a. the contract, agreement, or arrangement will provide for U.S. Government storage or storage by a cleared contractor at or near the delivery point. U.S. classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading. Any storage facility used or designated for this purpose must afford the U.S. classified material the protection required by this directive.

2.13.4 If U.S. classified material is to be delivered to a foreign government within the recipient country, it shall be transmitted in accordance with this chapter. Unless a designated or approved courier or escort accompanies the material, it will, upon arrival in the recipient country, be delivered to a U.S. Government representative who will arrange for transfer to an authorized representative of the recipient foreign government.

2.14 Receipt System

2.14.1 Top Secret material shall be transmitted under a continuous chain of signed receipts.

2.14.2 Secret and Confidential material shall be covered by a receipt between installations and other authorized addressees outside of NASA.

2.14.3 Receipts shall be provided by the transferring installation, and the forms will be attached or enclosed in the inner envelope or cover. Domestic Return Receipt form, PS Form 3811, or NASA Form 387 (Classified Material Receipt) or a facsimile will be used for this purpose.

2.14.4 Receipt forms shall be unclassified and contain only information necessary to identify the material being transmitted.

2.14.5 A duplicate copy of the receipt shall be retained in a suspense file until the signed original is returned. If a signed receipt is not received within 45 days, follow-up action will be initiated and the cognizant CCPS/CCS will be informed.

2.14.6 Copies of signed receipts shall be retained for a period of five years.

2.15 Managing and Handling COMSEC Material and Devices

2.15.1 COMSEC requires a higher order of protection given the classification of collateral Top Secret, Secret, and Confidential information. The definition of COMSEC deals with the measures and controls taken to deny unauthorized individuals information derived from the telecommunications and to ensure the authenticity of such telecommunications. Communication Security includes crypto security, transmission security, emission security, and physical security of COMSEC material. Pending issuance of separate specific NASA COMSEC policy and procedures, users of COMSEC material shall follow the requirements in managing and handling COMSEC material established in the NASA COR COMSEC Standard Operating Procedures (CSOP) and the National Security Telecommunications Systems Security Instruction 4005 (NSTISSI/CNSSI 4005). The Center COMSEC Officer will serve as the focal point for all COMSEC issues. The Center COMSEC Account Manager (CAM) and Alternate CAM serve as the focal point for all Center COMSEC issues. Contact the NASA COR for clarification of any COMSEC related issues, questions, and/or written approval and waivers to COMSEC policy (such as carrying COMSEC material and devices overseas, et. al.).

2.16 Defense Courier Service Reimbursement Program

2.16.1 Upon request of the AA for Protective Services, the CCPS/CCS shall provide information on the Center's use of the reimbursable service of the Defense Courier Service for transmitting CNSI outside the Center.

2.17 Disposition or Destruction of Classified Material

2.17.1 Inactive CNSI shall be disposed of in accordance with NPR 1441.1, NASA Records Retention Schedules. Each Center will employ security procedures and methods for destruction, witnessing, certification, and retention of CNSI in accordance with this chapter.

2.17.2 Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information.

2.17.3 Centers and other NASA Installations shall continuously review their classified holdings. Classified information will be destroyed when determined to be no longer required for operational or administrative purposes. The Center CCPS/CCS will establish annual Center-wide classified material destruction events to ensure classified holdings are properly reviewed and unneeded CNSI disposed of in accordance with NPR 1441.1. Prior to any classified information or document being disposed of, the Center Records Manager and the organization that controls the document, in coordination with the Center Protective Services Office, will determine whether or not the record is a permanent or temporary document, which will determine the disposition of the document. Once the document has been labeled as temporary or permanent, the record will be destroyed or sent to the NASA Records Center or the NARA for storage. Collecting or hoarding CNSI is prohibited.

2.17.4 Additional policy must be followed when destroying COMSEC material as contained in approved COMSEC Standard Operation Procedures and NSTSSI 4005.

2.17.5 Unclassified material, including formerly classified material that has been declassified and unclassified messages, does not require the same assurances of complete destruction. To avoid overloading an installation's classified material destruction system, unclassified material shall be introduced only when the CCPS/CCS or higher authority requires it because of unusual security considerations or efficiency.

2.17.6 Approved destruction methods. Destruction devices must be approved by the National Security Agency (NSA), as listed in NTISSI 4004 Annex B, NSA Evaluated Destruction Devices.

Pulpers, pulverizers, or shredders may be used for the destruction of paper products and some forms of computer media. Only paper-based products shall be destroyed by pulping. Classified material in microform, that is, microfilm, microfiche, or similar high-data density material, will be destroyed by burning or chemical decomposition or other methods as approved by the cognizant CCPS/CCS. Equipment approved for the destruction of classified material will be operated properly and provided with regular maintenance, as suggested by the manufacturer. The following are the approved methods for the destruction of classified material:

- a. Burning. When burning is used for destruction of classified information, ensure that the wind or draft does not carry portions of burned material away and that the resulting ash is broken up sufficiently to preclude reconstruction.
- b. Shredding. Any crosscut shredder whose residue particle size is equal to or smaller than 1/32 of an inch in width by 1/2 inch in length (1/32 x 1/2 is approved for the destruction of all classified paper material, magnetic tape, and cards. Shredders shall not be used to destroy classified microfilm, microfiche, or similar high-information density human readable material. This does not include COMSEC items, which must be destroyed in accordance with established NSA requirements contained in Committee on National Security Systems (CNSS) Policy No. 16, dated October 2002. These NSA requirements will be maintained at the Center Security/Protective Services Office.
- c. Pulping (Wet Process). Wet process pulpers with a 1/4 inch or smaller security screen shall be used to destroy classified water-soluble material. Since pulpers only destroy paper products, staples, paper clips, and other fasteners will be removed to prevent clogging the security screens.
- d. Pulverizing (Dry Process). Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use, unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators may be used to destroy photographs, film, typewriter ribbons, magnetic tape, flexible diskette (floppy disk), glass slides, and offset printing plates. Pulverizers and disintegrators shall have a 3/32-inch or smaller security screen.
- e. Chemical Process. Classified microfilm or microfiche shall be destroyed by chemical process.

2.17.7 Destruction of Classified Equipment. All components of classified equipment shall be destroyed by any method that destroys them beyond recognition.

2.17.8 Eradication of Magnetic Media. Destruction of classified Automated Information System magnetic media shall be in accordance with NSA/Central Security Service Policy 9-12, Storage Device Declassification Manual, and established NASA COMSEC requirements. A record of destruction records must be executed upon eradication of the classified information.

2.17.9 The Center Protective Services Office will provide specific guidance on how to destroy newer forms of media as required.

2.18 Destruction Procedures

2.18.1 Classified material shall only be destroyed by authorized means by individuals cleared to the level of the material being destroyed. A minimum of two individuals will be responsible for destroying Top Secret material and a minimum of one for Secret and Confidential. These individuals must have a need to know and must be authorized to destroy the material.

2.18.2 The personnel tasked with the destruction or preparation for destruction of classified material shall be thoroughly familiar with the requirements and procedures for safeguarding classified information. They will be thoroughly briefed on the following:

- a. Safeguarding all classified material entrusted to them for destruction.

- b. Conducting a thorough page check of Top Secret material before destruction is accomplished.
- c. Observing all documents destroyed or being prepared for destruction and checking the residue of locally destroyed material to ensure that destruction is complete and reconstruction is impossible.
- d. Taking precautions to prevent classified material or burning portions of classified material from being carried away by wind or draft.
- e. Completing and signing all appropriate records of destruction.

2.18.3 Classified waste shall be destroyed as soon as practicable. Containers used for the accumulation of Secret classified waste will be dated when the first item of classified waste is deposited. If, after 30 days, the classified waste has not been destroyed, a review will be conducted to determine why the information is still being stored and arrangements should be made immediately to destroy the material. When destruction is completed, a record of destruction will be prepared.

2.18.4 The CCPS/CCS shall review or direct a review, at least annually, of Center classified material holdings expressly for the purpose of reducing to an absolute minimum the quantity on hand.

2.19 Security Violations and Compromise of CNSI

2.19.1 The CCPS/CCS shall ensure that written procedures exist for the following:

- a. Emergency action and reporting requirements for the loss of CNSI.
- b. Action to be taken by the CCPS/CCS in the event of the loss of control over CNSI.
- c. Action required in the event that the lost CNSI was not compromised.
- d. Action required in the event of possible compromise of CNSI.
- e. Action required in the event of unauthorized disclosure of CNSI by NASA or contractor personnel.
- f. Notifying the OPS Security Management Division Director, the Central Adjudication Facility (CAF), and, as appropriate, Center management officials when classified information is presumed compromised.

2.19.2 A written incident report shall be made to the OPS Security Management Division Director on all issues as described in 2.19.1.

2.19.2.1 An initial report of incidents involving classified material requires an immediate notification and presentation of the facts for the purpose of limiting and assessing the damage to the national security. The initial report shall be made to the OPS Security Management Division Director within two working days. The intent is to notify all critical officials as soon as possible to limit further damage, assess weaknesses, and correct a discrepancy, if appropriate. If a formal report cannot be accomplished in two working days, the OPS Security Management Division Director will be provided with electronic mail that briefly describes the incident, immediate actions taken, and those planned. When a security incident involves the simultaneous compromise of CNSI, sensitive but unclassified information, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), etc., the Information Security Specialist will take the lead since the CNSI is the highest level of information involved in the incident. A team will be formed consisting of the Center Privacy Manager, ITAR/EAR Manager, and the Center, Chief Information Officer Representative to handle and coordinate the other information that falls outside the CNSI arena.

2.19.2.2 Immediate reports of incidents involving classified information shall contain the following information:

a. Type of report:

- (1) Compromise.
- (2) Possible compromise.
- (3) Administrative discrepancy.

b. Type of incident:

- (1) Compromise.
- (2) Possible compromise.
- (3) Improper destruction.
- (4) Unauthorized access.
- (5) Improper transmission (transmission via non-secure means or use of unauthorized equipment).
- (6) Improper storage.
- (7) Loss of material.
- (8) Found material (material not in accountability system or previously reported as lost) not subjected to possible compromise.
- (9) Other (explain).

c. Administrative discrepancy:

- (1) Mailed via non-registered/certified mail.
- (2) Sent in single container.
- (3) Markings on outer container divulged classification of contents.
- (4) Classification not marked on inner container.
- (5) No return receipt.
- (6) Inadequate wrapping: not securely wrapped or protected.
- (7) Received in poor condition: compromise improbable.
- (8) Addressed improperly.
- (9) Classified by unauthorized original classifier.
- (10) Markings incorrect.
- (11) Classified by, reason for classification, or declassify on, incorrect or missing (originally classified documents).
- (12) Derived from or declassify on line incorrect or missing (derivatively classified documents).
- (13) Other (explain).

d. Complete identification of all material involved including:

- (1) Unclassified title.
- (2) Classification.
- (3) Originator.

e. Identity of all personnel involved including:

- (1) Full name.
- (2) Social Security Number.
- (3) Security Clearance.
- (4) Basis of Security Clearance.

f. A statement of actions taken upon discovery of incident and description of events.

g. Weakness leading to the incident.

h. Corrective actions taken and actions taken to preclude recurrence.

i. Disciplinary action taken, if any.

j. Unit incident number, to include:

- (1) Fiscal year.
- (2) Sequential number.

2.19.2.3 The CCPS/CCS shall submit a final incident report within 30 days of the incident. The report will include:

- a. Likelihood CNSI was compromised (provide details supporting determination).
- b. General comments (may include authority to remove material from accountability or request further information).
- c. Incident closure or further investigation required.
- d. Center incident number (to include fiscal year and sequential number).

2.20 CNSI Meetings and Symposia

2.20.1 General.

2.20.1.1 Any meeting (conference, seminar, and exhibit) or symposium sponsored by NASA or held at a Center or NASA Headquarters where classified information is disclosed must meet the minimum-security standards established in paragraph 2.20.3. Meetings held by an association, society, or other group whose membership consists of primarily cleared contractors may be sponsored by NASA, provided that the contractor has an authorized contract in place and that an appropriately cleared contractor is designated and accepts responsibility for furnishing all symposium security measures.

2.20.2 Responsibilities.

2.20.2.1 Key officials of the Office of the Administrator, Officials-In-Charge of Headquarters Offices, and Center Directors are responsible for ensuring that the CCPS/CCS or the OPS Security

Management Division Director approval is obtained for a NASA-sponsored conference or symposium involving CNSI discussion and presentations. Security approval shall be coordinated with the Office of International and Interagency Relations regarding the attendance of any foreign nationals or representatives at a CNSI symposium or meeting.

2.20.2.2 The CCPS/CCS is responsible for ensuring that all minimum security standards are met.

2.20.3 Minimum Standards.

2.20.3.1 A CNSI meeting or symposium shall be restricted to appropriate areas at Government facilities approved for CNSI discussions or appropriate cleared contractor facilities.

2.20.3.2 Supervisors and meeting hosts shall ensure that all attendees possess the appropriate personnel security clearances and a need-to-know.

2.20.3.3 A request for security approval for a CNSI symposium shall be forwarded through the CCPS/CCS to the OPS Security Management Division Director. It will include the following items: date(s) and specific location for the proposed meeting (Government or cleared contractor facility), identification of CNSI subject matter and highest classification level involved, and the identification and status of any non-U.S. citizen (Foreign National or resident alien) and foreign representative invited to attend during any classified or unclassified session.

2.20.3.4 If any non-U.S. citizen, foreign national (to include resident aliens), or foreign representative shall be in attendance, the following information must be submitted to the OPS Security Management Division Director: complete name, date, place of birth, current citizenship status, type of personnel security clearance (if any), identification of each foreign government and/or entity represented, date(s) of attendance, nature of participation, and the reason why attendance is considered to be in the U.S. national interest.

2.20.3.5 Foreign nationals or representatives shall not be extended an invitation to attend or be permitted to attend any CNSI or unclassified session unless advance approval has been obtained from the OPS Security Management Division Director. Refer to NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA Installations or U.S. Citizens who are Representatives of Foreign Entities, for more detailed requirements on facilitating foreign national visits.

2.20.3.6 The CCPS/CCS or staff shall conduct a visual and physical inspection of the meeting room to help preclude any unauthorized disclosures of classified information.

2.21 Security Containers and Vaults

2.21.1 Deployment, use, and maintenance of security containers, vaults, and secure areas designed for storage or daily use and discussion of CNSI shall be centrally managed by the CCPS/CCS to ensure their use is consistent with Agency and Center policies and procedures for storage and accountability of CNSI. The CCS will:

a. Ensure only General Service Administration approved security containers, designed specifically for storage of CNSI, are used for the storage of Top Secret information. (Note: Non- General Service Administration approved containers may not be used for the storage of Secret or Confidential information after October 1, 2012, per ISOO memorandum dated, September 14, 2009).

b. Maintain a current database of all Center-wide security containers and vaults to include (at a minimum):

(1) Assigned Center-specific security container or vault.

(2) Location of container or vault.

(3) Custodian/Alternate custodian.

(4) Highest classification level of information stored.

c. Ensure approved containers and vaults are used only for storage of CNSI and necessary unclassified reference materials. Storage of unclassified materials must be kept to the absolute minimum.

d. Ensure high-value items that are targets of theft such as funds, weapons, and precious metal are not to be stored in the same drawer as classified materials.

e. Ensure approved security containers and vaults are appropriately decertified and properly tagged "Not for Storage of Classified Material" by the CCPS/CCS prior for use in storage of non-classified material.

f. Establish procedures to remove unneeded security containers that are removed from service and retained for future use or properly disposed of.

g. Ensure locking mechanisms are properly outfitted with or upgraded to appropriate Federally mandated "X" series locks under the following circumstances:

(1) When the security container or vault is newly procured or reentered into service. (NOTE: For storage of classified material: containers and vaults must be inspected, reconditioned as necessary, recertified, and designated in writing by the Center locksmith and acknowledged by the CCPS/CCS prior to being reentered into service.)

(2) When the locking system requires replacement.

(3) When, at the discretion of the CCPS/CCS, funding is available to retrofit existing container or vault inventory.

(4) When the container or vault is used to store Top Secret, COMSEC, Special Access Required, or SCI information and material.

2.22 Security Areas

2.22.1 Types of Secure Areas.

2.22.1.1 Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource shall be "Restricted" areas (as a minimum designation).

2.22.1.2 Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors shall be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

2.22.1.3 Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

2.22.2 All plans for secure areas must be submitted and approved to the OPS Security Management Division Director before classified material can be stored in that area.

2.23 Classified Material Is NOT Personal Property

2.23.1 Classified information is always official U.S. Government information and never your own personal property. Confusion sometimes arises about classified notes from a training course or conference. As classified material, it is official information that must be safeguarded, transmitted, and destroyed in accordance with this NPR. Classified notes cannot be removed from a NASA installation without the approval of the Center Director or CCPS/CCS. Classified notes shall not be considered as working papers but as official information for which the Center/facility is responsible. It must be transmitted by one of the means authorized for transmittal of classified material and eventually destroyed by authorized means. When an individual leaves one NASA installation and transfers to another, the installation may officially transfer his/her notes as classified material to the new NASA installation where the material will again be available for his/her use. If the individual desires to have the material transferred to another U.S. Government agency, the CCPS/CCS, as approved by the Center Director, may facilitate such transfers.

2.23.2 CNSI is always the property of the United States Government. Individuals who remove CNSI may be subject to disciplinary action up to and including criminal prosecution under Titles 18 and 50 of the United States Code and other applicable laws.

2.24 Security Classification Reviews for NASA Programs and Projects

2.24.1 Pursuant to NPR 7120.5, NPR 7120.7, and NPR 7120.8, programs and projects must conduct formal security reviews that, in addition to personnel, physical, and information technology security, shall include reviews for traditional information classification security needs. Security reviews will be undertaken to determine if information used or produced as part of a program or project, meets the requirements for designation as CNSI controlled information. Program and project managers will contact their local Center Protective Services Office for classification assistance at the beginning of all new projects as required. Project managers will:

- a. Complete NASA Form 1733, Information and Technology Classification and or Sensitivity Level Determination Checklist. The local Center Security Protective Services Office Information Security Specialist should be consulted for assistance with this form and the classification process.
- b. Take the completed form to the Center Protective Services Office for review and approval.
- c. Include the Form 1733 as permanent program documentation and in any procurement-related documentation.

2.24.2 Upon the conclusion of the security review, if the information surrounding or concerning the program or project, or portions thereof, meet one or more of the categories of information presented in Exec. Order No. 13526, a subject matter expert (SME) with assistance from the CCPS/CCS must develop an appropriate SCG. The SME and project officials shall consider the level of classification needed for specific information. APPENDIX A provides a definition of each. SMEs must be able to specifically identify what particular information is under consideration for classification. The SME, weighing the information being protected against the definitions in APPENDIX A, will provide a recommendation to the OPS as to what level the information must be classified (Top Secret, Secret, or Confidential) and how long the information must be kept classified. Duration of classification will be considered within the following guidelines:

- a. The SME shall attempt to determine a date or event that is less than 10 years from the date of original classification and that coincides with the lapse of the information's national security sensitivity and will assign such date or event as the declassification instruction.
- b. If unable to determine a date or event of less than 10 years, the SME shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

c. If unable to determine a date or event of 10 years, the SME shall assign the declassification date not to exceed 25 years from the date of the original classification decision.

2.24.2.1 All SCGs must be approved by the OPS. The CCPS/CCS and the OPS Security Management Division Director shall assist program and project managers in the development of SCGs.

2.24.2.2 The OPS will establish and maintain a central repository for all NASA-originated SCGs and declassification guides and shall provide a sequential numbering schema for all SCGs and declassification guides both classified and unclassified. The OPS will also obtain and maintain SCGs and declassification guides from other Agency programs in which NASA is working or supporting. The CCPS/CCS will provide the OPS Security Management Division Director an updated list of all SCG on their Center by September 30 each year.

2.24.2.3 The SCG must be reviewed for updating every 5 years.

2.24.2.4 Upon completion, termination, or cancellation of a program or project, a declassification guide must be produced to provide the necessary requirements for declassifying the project information. The declassification guide must be approved by the OPS. Section 2.2 of Exec. Order No. 13526 contains additional details pertaining to classification guides.

2.24.2.5 The "NASA Handbook for Writing Security Classification Guide" provides requirements and guidance for the creation of a SCG. The handbook is located in the OPS Information Security Program.

2.24.3 If information surrounding or concerning the program or project is considered to be unclassified, a letter of transmittal shall be produced that reflects this determination. The project office will maintain the original letter with copies sent to the appropriate responsible Mission Directorate and to the OPS Security Management Division Director.

2.24.4 All CNSI information should be reviewed by a record manager, the responsible program manager/office head, and a Declassification Authority (DCA), if the information is classified, to determine the disposition of the records before they are sent to the Federal Records Centers or the NARA for temporary or permanent storage.

2.25 Access to Classified National Security Information Granted by Another Government Agency

2.25.1 All NASA employees receiving access to classified information from agencies such as the Department of Energy, Department of Defense, National Security Agency, Department of Homeland Security, Nuclear Regulatory Agency, State Department or any other Government agency shall protect and control the classified information in accordance with the regulations and policies provided to them by the agency granting the access and need to know. The employee must contact their NASA Center Protective Service Office to receive assistance with safeguarding and protecting the information if they are required to maintain the classified information at a NASA Center, Component Facility, or location.

2.26 Special Access Program (SAP)

2.26.1 A SAP shall be created within NASA only upon specific written approval of the Administrator and coordinated with the Office of Protective Service Intelligence Division Director to ensure required security protocols are implemented and maintained. The Administrator, along with SAO and the Office of Protective Services Intelligence Division Director, reviews each SAP annually to determine whether it continues to meet the requirements of Exec. Order No. 13526.

2.26.2 All personnel security requirements for NASA personnel to establish and participate in

SAP external to NASA must be coordinated with the OPS Intelligence Division Director to ensure accountability of NASA equities.

2.26.3 All NASA security activity associated with SAPs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG). All NASA SAPs will adhere to the standards in the SAPSG.

2.27 Sensitive Compartmented Information (SCI) Programs

2.27.1 SCI programs shall only be created within NASA upon specific written approval of the Administrator and coordinated with the OPS Intelligence Division Director to ensure required security protocols are implemented and maintained.

2.27.2 All requests for NASA personnel, including NASA contractors, to participate in SCI programs external to NASA must be coordinated with the OPS Intelligence Division Director to ensure accountability of NASA equities.

2.27.3 Failure to comply with the requirements of this section may result in denial of security clearance and suspension of SCI activity.

2.28 Industrial Security

2.28.1 General.

2.28.1.1 This chapter provides procedural requirements for implementation of the industrial security program in accordance with the National Industrial Security Program Operating Manual (NISPOM).

2.28.1.2 Industrial security pertains to, but is not limited to, the requirement to review all programs/projects in accordance with associated regulations, classified contract administration rules and requirements, and the processing and control of classified visits for cleared Government and contractor employees.

2.28.1.3 This chapter is applicable to contracts, grants, cooperative agreements, and other binding transactions in which performance shall require access to CNSI by the contractor, supplier, grantee, or its employees. It does not apply to agreements with other Federal agencies.

2.28.1.4 The processing and control of classified and unclassified visits to a Center in relation to classified contracts is the responsibility of the CCPS/CCS and shall be covered in written local security procedures tailored to that Center.

2.28.2 DoD Support

2.28.2.1 The Defense Security Service (DSS) administers the National Industrial Security Program on behalf of NASA. This support extends to contractor sites. The CCPS/CCS is responsible for oversight of industrial security services of contractors on NASA Centers and facilities, excluding personnel security clearances.

2.28.2.2 The standard security provisions of NASA classified contracts require the contractor to possess a facility security clearance (FSL) and be assigned a CAGE code, execute a DoD Contract Security Specification (DD Form 254), and complete other applicable industrial security forms that require the contractor to comply with the NISPOM for industrial security matters. If the prime contractor does not possess a facility security clearance, the CCPS/CCS will request, through DSS, that a facility security clearance be issued in accordance with the NISPOM.

2.28.2.3 NASA shall exercise its right as documented in contracts, to inspect contractor operations located on NASA property that are involved in accessing and safeguarding classified information.

This review must be documented on the Department of Defense DD-254 Form and within the contract specifications.

2.28.3 Responsibilities.

2.28.3.1 NASA program or project management personnel contemplating offers or quotations for a classified contract, negotiating or awarding a classified contract, or bearing responsibility for the performance of a classified contract shall:

- a. Ensure the CCPS/CCS is fully engaged in supporting the development of security requirements for the contract.
- b. Ensure adequate resources are provided to the CCPS/CCS for program security oversight, as required.
- c. Pursuant to the NISPOM, ensure the contractor provides a "Classified Visit Request" to the CCPS/CCS with a list of all the contractors and their clearance level. The contractor shall provide the CCPS/CCS an updated list when a contractor is added or deleted from the contract.

2.28.3.2 The Director of Procurement of each Center is responsible for the following:

- a. Ensuring that the request for proposals or offers includes a statement that the contractor or prospective contractor will or will not require access to classified information and will or will not generate classified information in the performance of such contract. If the contract shall involve access to classified information or cause the generation of classified information, a letter requiring each contractor shall comply with the National Industrial Security Program Operating Manual (NISPOM) as required, will be attached to the material submitted to the individual negotiating the contract.
- b. Ensuring that each classified contract contains the standard security clauses prescribed by the NASA Far Supplement Part 5200-11, Subpart 1852.204-75-Security Classification Requirements as prescribed in 1804.404-70 for classified contract requirements.
- c. Ensuring that any proposed deviation in this standard security provision (elimination, addition, or substitution) is forwarded to the Office of Procurement for approval by the Assistant Administrator for Procurement, with concurrence by the AA for Protective Services and the NASA Office of General Counsel (OGC).

2.28.3.3 The CCPS/CCS shall ensure that NASA recommendations affecting the contractor's security program are made primarily through the cognizant security office DSS for the contractor concerned, since DSS is primarily responsible for ensuring that the contractor complies with all security recommendations. When it becomes apparent that full and satisfactory action on a specific NASA recommendation has not been taken by the cognizant security office or by the contractor, a detailed report of the circumstances will be forwarded to the AA for Protective Services for appropriate action with a copy to the contracting officer.

2.28.3.4 All changes to a contractor's security program that may affect the cost, performance, or delivery of the contract must go to the contracting officer through processing of a contract modification.

2.28.3.5 Through coordination with the contracting officer and contracting officer's technical representative, the CCPS/CCS shall develop local written security procedures to ensure that the following requirements are met:

- a. The NASA contracting officer has the responsibility to include the DD 254 in the Request For Proposal (RFP) and contracts. The Center Security Office has the responsibility for generating the

DD-254 and signing the document. Center Security must review the RFP and/or contract to fully understand the requirements and implications of the procurement action with regard to security.

b. In item 12 of the DD Form 254, delete the words: "To the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review in accordance with the Industrial Security Manual," and insert the words: "To the Office of Communications, National Aeronautics and Space Administration, Washington, DC 20546, for review."

c. In the case of prime contracts, the Office of Communications Public Information Office of the NASA contracting Center shall also be specified in item 12 to indicate that proposed publicity releases will be submitted through that office to the Office of Communications.

d. In the case of subcontracts, the publicity office of the prime contractor shall be specified, in addition to the Office of Communications Public Information Office of the NASA Contracting Center, to indicate that proposed publicity releases will be submitted through those two offices to the NASA Office of Communications.

2.28.3.6 The CCPS/CCS shall ensure contractors operating under a DD Form 254 provide the appropriate "Classified Visit" documentation, pursuant to the NISPOM, on all "cleared" contractor personnel working under the DD Form 254 and ensure updates are provided on an as needed basis. Classified visit requests are mandatory for all NASA Classified Contracts.

2.28.4 Suspension, Revocation, and Denial of Access to Classified Information.

2.28.4.1 Center security offices may find it necessary to take action to suspend, or deny a NASA contract employee's access to CNSI or, in coordination with the NASA contracting officer, to suspend operation of the entire contract. To ensure uniformity and consistency, the following shall apply:

a. In the rare cases NASA has granted a contractor's clearance, only the AA for Protective Services or designee may deny or revoke a cleared contractor's access to classified information.

b. The AA for Protective Services, Center Director, CCPS/CCS, or the OPS Security Management Division Director shall suspend a contractor's access for cause.

2.28.4.2 Each action shall be fully documented. Information developed during the security inquiry will not be shared with the contracting officer or contractor management while the inquiry is ongoing. The Office of Protective Service/Director for Security Management Division or CCPS/CCS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, is a threat to a critical mission, or may otherwise be ineligible for continued access to classified information.

2.28.4.3 Center security officials shall ensure coordination is effected with the local or regional Industrial Security investigative organization (OPM and DSS) to obtain direction and to ensure information is provided to enable them to properly adjudicate for continued clearance eligibility.

2.28.4.4 During the investigative and adjudicative process, all reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

2.28.4.5 The CCPS/CCS shall propose denials and revocations of contractor access to the AA for Protective Services. The AA for Protective Services will make final denial or revocation determinations after consultation with the NASA Central Adjudication Facility and the OGC.

2.28.4.6 Subjects of adjudication must be allowed to review and refute any information developed

during the investigation process that shall make him or her ineligible for access to NASA CNSI, unless release of that information jeopardizes national security.

2.28.5 Periodic Review of DD Form 254.

2.28.5.1 Each approved DD Form 254, Contract Security Classification Specification, or other written notification, issued in lieu thereof, shall be reviewed at least annually by CCPS/CCS with the assistance of the procurement office.

2.28.5.2 The individual(s) responsible for this review shall be identified by the CCS in local written security procedures.

2.28.5.3 When a change is made in a security classification specification pertaining to a prime contract, that change shall be reflected in all applicable Form DD 254s or other classification documents pertaining to subcontractors.

2.29 Information Systems Security of CNSI

2.29.1 Information systems (IS) that are used to capture, create, store, process, or distribute CNSI must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system. The OPS shall be responsible for the certification and accreditation for all NASA Classified National Security Information (CNSI) systems, networks, and Protected Distribution Systems.

2.29.2 Protection requires a balanced approach, including information systems security features to include, but are not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the information systems are required. Information shall not be downloaded onto memory sticks, jump drives, USB flash drives, or any other type of device without specific documented approval from the information system owner or the authorized security official that controls access to the system.

2.30 ISOO Reporting Requirements

2.30.1 The OPS is responsible for completing the following annual reports from ISOO in accordance with Exec. Order No. 13526:

- a. ISOO Agency Security Classification Management Program Data (SF-311).
- b. ISOO Annual cost Estimates for Security Classification Activities (SF-716)..
- c. ISOO Senior Official Self-Inspection Program Report.
- d. Fundamental Classification Guidance Review.
- e. Security Violations and Sanctions. In accordance with Section 5.5 of Exec. Order No. 13526, the OPS will report to ISOO any violation or sanction that is prohibited by the Executive Order.

Appendix A: Definitions

Access. The ability or opportunity to gain knowledge of classified information.

Adjudication. A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources, is in the best interest of national security or efficiency of the Government.

Authorized holder. Anyone who satisfies the conditions for access to classified information in accordance with section 4.1 (a) in Exec. Order No. 13526.

Automatic declassification. The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority or the expiration of a maximum timeframe for duration of classification established under Exec. Order No. 13526 .

Center Chief of Security (CCPS/CCS). The senior Center security official responsible for technical management of the Center security program.

Central Adjudication Facility (CAF). Facility established at the Security Management Division-level which is responsible for adjudicating all requests for clearances to access CNSI.

Certification. A formal process used by the Certifying Official to ensure that an individual has met all established training requirements necessary to perform their security responsibilities.

Classification. The act or process by which information is determined to be classified information.

Classification guidance. Any instruction or source that prescribes the classification of specific information.

Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified Material. Any physical object on which is recorded or in which is embodied CNSI that must be discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information (CNSI). Information that must be protected against unauthorized disclosure in accordance with Exec. Order No. 13526, "Classified National Security Information," as amended and is marked to indicate its classified status when in documentary form.

Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

Collateral Classified. All CNSI, excluding information in the SCI or SAP information category.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Compilation. An aggregation of preexisting unclassified items of information.

Compromise. The improper or unauthorized disclosure of or access to classified information.

Contractor. For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

Damage. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification. The authorized change in the status of information from classified information to unclassified information.

Declassification Guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Declassification Authority (DCA). An official delegated declassification authority in writing by the Agency head or the SAO.

Denial. The adjudication that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in Exec. Order No. 13526 have been exercised.

Derivative classification. The incorporation, paraphrasing, restating, or generation of a new form of information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading. A determination by a declassification authority that information classified and safeguarded at a specified level must be classified and safeguarded at a lower level.

Escort. A NASA civil service employee or contractor responsible for the management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training includes the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, and authorized topics of discussion.

File Series. File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Foreign Government Information. (1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence. (2) Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence. (3) Information received and treated as foreign government information under the terms of a predecessor order.

Foreign National. For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful

permanent resident (i.e., holders of green cards) or persons admitted with refugee asylee status to the United States.

Formerly Restricted Data (FRD). Defined by the Atomic Energy Act as classified information which has been removed from the RD category after DOE and the DOD have jointly determined that it relates primarily to the military's utilization of atomic weapons and can be adequately safeguarded as national security information.

Information Security Oversight Office (ISOO). Office established under the Executive Office of the President tasked with policy development and oversight of Federal agency compliance with national-level policy for management of CNSI.

Intergovernmental Personnel Act (IPA). Individuals on temporary assignments between Federal agencies and state, local, and Indian tribal governments, institutions of higher education, and other eligible organizations. IPAs can include foreign nationals.

Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors must be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

Mandatory Declassification Review. The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of Exec. Order No. 13526.

NASA Employee. NASA civil service personnel.

National Security. The national defense or foreign relations of the United States.

National Security Position. Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

Confidential. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the Original Classification Authority is able to identify or describe.

Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the Original Classification Authority is able to identify or describe.

Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

Need-to-Know. A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Nondisclosure Agreement. Standard Form 312 (SF 312) is a non-disclosure agreement required under Exec. Order No. 13292 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the ISOO of the NARA and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. The SF 312 replaces the earlier forms SF 189 or the SF 189-A. Enforcement of SF 312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion, or

removal, in addition to the likely loss of the security clearance."

Original Classification. An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

Original Classification Authority (OCA). An individual authorized in writing, either by the President, by agency heads, or other senior Government officials designated by the President, to classify information in the first instance.

Page Check. Involves visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the original document. In the absence of a list of effective pages, the document will be examined for continuity.

Permanent Resident Alien. A non-U.S. citizen legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 3 C.F.R, Part 7, Section 7.4), and access to CNSI. Permanent Resident Aliens are not prohibited from accessing export controlled commodities, but must still have a work-related need-to-know and are still considered foreign nationals under immigration laws.

Records. The records of an agency and Presidential papers or records, as those terms are defined in 44 U.S.C. § 2905, § 3101, and § 3102, including those created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant. Records having permanent historical value include Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with 44 U.S.C. § 2905, § 3101, and § 3102.

Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource must be "Restricted" areas (as a minimum designation).

Restricted Data (RD). Defined by the Atomic Energy Act as all data concerning design, manufacture, or utilization of atomic weapons, production of special nuclear material, and use of Special Nuclear Material in the production of energy.

Safeguarding. Measures and controls that are prescribed to protect classified information.

Security Classification Guide. The written direction issued or approved by a Top Secret/OCA that identifies the information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material.

Security Clearance. A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to national security.

Security Management Division Director. Official assigned to the OPS who is responsible for Agency management of physical security, industrial security, program security, and NASA Federal Arrest Authority and Certification.

Self-inspection. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under Exec. Order No. 13526 and its implementing directives.

Senior Agency Official (SAO). The official designated by the agency head under section 5.4 (d) of Exec. Order No. 13526 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Sensitive Compartmented Information (SCI). Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

Source Document. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP). Any program established and approved under Exec. Order No. 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Suspension. The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with 44 U.S.C. § 2905, § 3101, and § 3102.

Unauthorized Disclosure (Exec. Order No. 13526). A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

Waiver. The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

Appendix B: Acronyms

AA	Assistant Administrator
APO	Army Post Office
CAM	COMSEC Account Manager
CAF	Central Adjudication Facility
CAGE CODE	Commercial and Government Entity Code
CCPS	Center Chief of Protective Services
CCS	Center Chief of Security
C.F.R.	Code of Federal Regulations
CMCO	Classified Material Control Officer
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CNSSI	Classified National Security System Instruction
COMSEC	Communications Security
COR	Central Office of Record
CSOP	Central Office of Record Standard Operating Procedures
DCA	Declassification Authority
DCP	Document Control Points
DCS	Defense Courier Service
DCSO	Document Control Station Official
DOD	Department of Defense
DOE	Department of Energy
DSS	Defense Security Service
EAR	Export Administration Regulation
FedEx	Federal Express
FGI	Foreign Government Information
FPO	Fleet Post Office
FRD	Formerly Restricted Data
IPA	Intergovernmental Personnel Act
IS	Information Systems
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office

ITAR	International Traffic in Arms Regulation
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NASA	National Aeronautics Space Administration
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSA	National Security Agency
NSTISSI	National Security Telecommunications Information Systems Security Instruction
OCA	Original Classification Authority
OGC	Office of General Counsel
OPM	Office of Personnel Management
OPS	Office of Protective Services
RD	Restricted Data
SAO	Senior Agency Official
SAP	Special Access Program
SAPSG	Special Access Program Security Guide
SCG	Security Classification Guides
SCI	Sensitive Compartmented Information
SCP	Security Control Point
SF	Standard Form
SME	Subject Matter Expert
SSO	Special Security Officer
TSCO	Top Secret Control Officer
UCNI	Unclassified Controlled Nuclear Information
U.S.C.	United States Code
USPS	United States Postal Service

Appendix C: References

C1. Procedures, 50 U.S.C. § 435.

C2. Security Requirements for Government Employees, as amended Exec. Order No. 10450.

C3. Administrative Personnel Suitability Determination, 5 C.F.R. § 731.202.

C4. Personal Identity Verification (PIV) of Contractor Personnel, 48 C.F.R. Federal Acquisition Regulation Clauses 52.204-9.

C5. NPR 1382.1, NASA Privacy Procedural Requirements.

C6. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

C7. NASA Handbook for Writing Security Classification Guides.